TAB

DCI/ICS-83-4279
15 March 1983

STAT

MEMORANDUM FOR: [redacted]
Acting Director, Intelligence Community Staff

STAT

FROM: [redacted]
Director, Planning and Policy Staff

STAT

SUBJECT: [redacted]

Request you authorize the obligation of $83,200 in FY-83 ICS funds for a study contract with the [redacted] The draft proposal for this contract is attached. The purpose of this contract is to develop an Intelligence Community Action Plan for enhancing computer security. (C)

STAT

STAT

[redacted]

Attachment: a/s

STAT

APPROVED: [redacted]
Director, Intelligence Community Staff

3/22/83
Date

STAT

WARNING NOTICE
INTELLIGENCE SOURCES

[redacted]

Proposal for an IC Computer Security Project

I. Proposed Contractual Agreement

STAT

[redacted]

performance of work in support of this project subject to the written consent of the Contracting Officer and other applicable regulations.

II. Statement of Objectives

STAT

The Project Director, [redacted] will be responsible for achieving the Project Objectives assuming the level of IC participation and support described in Section III below.

The general scope of "computer" systems/networks and activities which may be covered by the recommendations and actions resulting from this project subject to agreement between the DCI and SECDEF is:

... All systems associated with classified intelligence information and with other classified Department of Defense information.

... Data security but not "COMSEC per se," TEMPEST, nor personnel and physical security for included systems.

Contractor computer systems/networks will be included to the extent they fall within the project's scope.

The Project Objectives (which will serve as individual task statements) are:

1. A continuing current Estimate of Vulnerabilities of included systems and activities sufficiently identified that the sources of threats and the associated risks can be cited and measured. There will be two such estimates made: the first will be more general for wide-audience use, while the second will be more specific designed for detailed discussion by a selected small IC audience.

2. An Assessment of Security Measures and Processes now in place within the Intelligence Community. This assessment will be specifically oriented towards the systems, networks, and activities included in the proposed project scope and will acknowledge the following assertions or problems:

ISSG
COMSEC
ODP
IMS

- Intelligence Community agencies or entities have or will have the responsibility for measuring and accrediting the security of individual computer systems, networks and activities included in project coverage.

- The increase in computer utilization has resulted in a large number of computer systems, etc., whose security is not fully known nor tested to approved joint DoD/DCI criteria.

- Security requirements of computer systems, etc., which are the responsibility of the Intelligence Community are presumed to be more demanding and more complex (e.g., compartmentation requirements) than those of the remainder of the USG and the private sector. Hence, a "buy" by the IC of commercial or other USG products (services) will probably not totally meet IC computer security requirements.

- A usable assessment can be made on the basis of a statistically significant set of examples and does not require a knowledge of all included computer systems, etc.

- There has been a recognized lack of resources applied to computer security; hence, the proposed assessment will serve to highlight known or perceived deficiencies.

SECOM

3. A Review and Delineation of Assigned Computer Security Responsibilities relevant to the activities within the scope of the project's attention. The pressure for this objective (task) arises from:

- A ten-year patchwork quilt of directives, organizational charters, and traditional individual agency actions which results in confusion on the part of users, "budget makers" and involved managers and which has hindered progress towards achieving adequate computer security.

- The large number of well-intentioned, highly motivated organizational entities with "assigned" responsibilities but without accompanying resources.

- The need to know the existing platform of competencies and assignments upon which a well-structured, understandable, and effective IC Computer Security policy and process can be built.

[illegible] for
[illegible]ment for
[illegible] briefing

4. A Computer Security Technology Needs and Assessment Statement to identify needed R&D projects and to identify where technology transfer can adequately serve the Intelligence Community. Computer security is an immature technology, and consequently there has been to date an inadequate compilation of IC technology requirements upon which focused "sized" R&D efforts can be funded. The present situation is typified by small, sometimes redundant projects which are unable to resolve the more critical high priority problems.

This objective (task) will rely heavily on work already done by, and information available from, CIA, DIA, NSA, OSD and the Military Departments/Services. Also, there are private sector and other USG organizations (e.g., NBS) which have excellent competencies and technical information available to the IC.

SECOM??

5. An IC Action Plan for Carrying Out Its Computer Security Responsibilities. This Action Plan will include:

- Mechanisms for maintaining current estimates of relevant vulnerabilities and threats.

- Proposed organizational assignments of responsibilities within the IC, DoD and, as appropriate, other USG agencies.

- A proposed mechanism for computer security assessment, certification and accreditation.

- A priority ordering of computer systems, networks and activities which should be addressed as to their computer security.

- A proposed coordinated computer security R&D program with a proposed continuing coordinating mechanism for a supportive R&D program/budget process.

- A policy framework for the establishment and maintenance of appropriate guidelines and regulations including DCID 1/16 and other instruments.

- A mechanism for a continuing on-going relationship with the R&D Community to facilitate communication and technology transfer.

6. A Draft Memorandum of Understanding (MOU) Between the DCI and SECDEF to guide IC and DoD computer security-related activities.

III. Government-Furnished Support

The Director of the IC Staff will assign or make available the equivalent of 2.5 IC Staff professional man years along with necessary cleared clerical help. In addition, the Director will arrange, as he believes necessary, for appropriate participation by the Defense Intelligence Agency (DIA), the Central Intelligence Agency (CIA), the National Security Agency (NSA), DoD (C^3I & P), the Military Departments and Services, and others.

Participation by non-Government consultants will be required. These consultants will provide written reports essential and contributory to the project and will participate in workshops and meetings as appropriate. To assure proper access and security controls, the IC Staff will directly fund for consultant participation. It is expected that one-half professional year equivalent of consultant support will be funded in this manner.

IV. Task Schedule

The following task schedule is proposed with all dates on an After Receipt of Order (ARO) base.

- Task 1: A Continuing Estimate of Vulnerabilities
  ... 90 days ARO
  This task will be performed primarily by IC analytic grou and is therefore not under the control of the Project Director. Nevertheless, the Project Director will support it the best of his/her ability and will structure work on the remaining tasks to be as independent of the completion date an quality of this task as possible.

- Task 2: Assessment of Security Measures and Procedures
  ... 180 days ARO

- Task 3: Review and Delineation of Assigned Computer Security Responsibilities
  ... 150 days ARO

- Task 4: Computer Security Technology Needs and Assessment Stateme
  ... 210 days ARO

- Task 5: An IC Action Plan for Carrying Out Its Computer Security Responsibilities
  ... 360 days ARO

- Task 6: A Draft MOU Between the DCI and SECDEF
  First draft .... 180 days ARO
  Final draft .... 360 days ARO

The task schedule assumes access to materials, documents and personnel agreed upon as being essential to task completion. The task schedule also assumes support by the IC Staff for workshops agreed upon as being essential to task completion.

V. Reporting Requirements

1. Written status reports covering progress to date, problems encountered, and the expenditure of funds will be provided on a bimonthly basis in the format prescribed by the COTR.

2. Reports will be provided upon completion of each Task.

3. Oral briefings will be made by the Project Director upon request of the COTR at dates mutually agreed upon.

4. The IC Staff will produce the required numbers of copies of the Reports submitted for distribution as it determines necessary.

5. Any changes to the proposed schedule will be requested by the Project Director at least ten working days ahead of the scheduled date for approval by the COTR or the Contracting Officer as appropriate.

STAT

VI. Compensation and Method of Payment

[redacted]

ROUTING AND TRANSMITTAL SLIP

Date

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. C/OS/ISSG		
2. [redacted]		
3.		
4.		
5.		

STAT

	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS Jim,

Attached are two drafts to replace [redacted] One was done by OSD/DOD and the other by NSA. The answers to the questions we talked about are:

STAT

a. Why? The IG/CM organizational study said all PD's should be reviewed. In addition, I understand that this was on Col. Wayne Kay's OSTP ~~(NSC)~~ plate for a long time before he left and in fact had a draft to President Carter before the latter left the White House. Old business.

b. Who directed? Partially explained above but the NCSC and COG (or all users of [redacted] believe it needs rehashing.

STAT

C. Next step? Wayne has another meeting scheduled for next Monday. The group plans to continue to massage this issue until ~~xx~~ they believe it is ready for review by all interested (over)

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
C/OC-CSD	Phone No.

5041-102

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆ GPO : 1981 O - 341-529 (120)

ADMINISTRATIVE - INTERNAL USE ONLY

ROUTING AND RECORD SHEET

STAT

SUBJECT: (Optional) Position Paper of the Office of Security on the Proposed [redacted]

STAT

FROM: [redacted]

8 SEP 1983

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. DD/P&M 4E63 Hqs				THE [redacted] STUDY IS UNDERWAY. SOURCES AND METHODS TYPE PROTECTION IS AT THE REAL ROOT OF OUR CONCERNS. AND WE HAVE UNIQUE PROBLEMS [redacted] IN CIA. 9/8/83
2.				
3. DD/Sec 4E63 Hqs				
4.				
5. D/Sec 4E63 Hqs				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

STAT

STAT

ADMINISTRATIVE - INTERNAL USE ONLY